kasada

CASE STUDY

How a large energy company drastically reduced fake traffic, fraud, and friction with Kasada

A leading integrated energy business in Australia with the largest private electricity generation portfolio, serves 3.7 million customers, including residential, small and large business, and wholesale customers.

As the online economy became increasingly bombarded by rampant malicious bot and scraper traffic in 2017, the energy organization sought to accelerate its digital transformation planning. In order to ensure that its accounts and IP were solidly protected and its platform fully optimized, the company turned to Kasada.

THE PAIN

The company was keeping a close watch on growing industry-wide online threats that could affect them—on one hand, payment fraud, and on the other hand, scraping (some of which was "generic vulnerability scanning" and some of which was much more insidious and elusive). The key concerns were to mitigate the risk of backend payment fraud at the payment gateway and to protect pricing IP on the quoting engine.

The business had done a proof of concept with a leading bot manager, largely centered on two business use cases. Firstly, they were looking at where they were exposing pricing information and how to protect its quoting from reverse-engineering on the pricing engine. Secondly, they sought to protect the payment gateway from fraudulent activity.

The energy company wanted to avoid a classic legacy scenario wherein relying on blunt controls such as WAF for geo-blocking leads to a constant cat-and-mouse game. The organization had found previous providers lacking in effectiveness and in their ability to explain problems, as well as being very expensive.

THE SOLUTION

To prevent unwanted traffic from reaching the threshold of unacceptable levels, the company knew it needed to act fast. Kasada provided immediate relief.

> "We were about to commence a POC with Kasada when we got hit hard by a large-scale automated attack, **said the CISO of the energy company.** "Slotting the technology in under an actual security incident and putting it through its paces proved what Kasada could do right out of the box. Instead of chasing after constantly morphing bots and scrapers, with Kasada we are able to use the crypto piece to smash that infrastructure—just blow them up. Essentially, we now have a deterrent control that inflicts a whole lot of pain on the bot and scrapers' backend and on their costs. They move on to an easier target."

kasada

> "Additionally, with cleaner traffic we were immediately able to identify poorly written applications and to solidify Request for Comment (RFC) standards throughout our channels," **said the CISO.** "Another benefit is analytics. Cleaner traffic means cleaner data. When you stop automated traffic from hitting backend servers, you get a better view of who your customers are and how much traffic is actually human. You get right-sizing on the backend, which gives you a better view of marketing. Prior to Kasada, it was a little bit all over the place. More accurate data enables a better view of site traffic and in turn enables you to work out target segments more effectively."

THE RESULTS

Since implementing Kasada, the energy company has realized multiple benefits including:

- Stopping attacks and having the control and flexibility to tune the product during attacks
- Having the ability to take swift and decisive action to remediate, rather than ride out problems with existing and pricey solutions, paying an even higher price later
- Exposing inadequate applications and ensuring RFC standards and best practices, triggering savings that paid for the product for five plus years forward
- Eliminating payment fraud at the gateway by constantly cleaning and washing away bad traffic, improving the customer journey without introducing latency
- Protecting pricing IP on the quoting engine by foiling reverse-engineering price scrapers
- Diminishing bot and scraper ROI, thereby conversely immediately improving in-house ROI
- Right-sizing traffic and thereby right-sizing backend resources
- Achieving clean data via triaging human versus synthetic traffic, thus enabling better market segmenting and more targeted marketing spend
- Being able to rely on solid, ongoing service and quality support by a solutions partner that proactively reaches out to provide help in shaping roadmaps and ensuring fast, needed outcomes

> "The number of transactions and dollar values we saved with Kasada were immediately apparent," **the CISO concluded.** "We've started to put Kasada across all our channels, across API, across mobile, across all the other areas including our customer identity system to protect against credential harvesting. So, while the initial use cases were business-driven, we've extended Kasada over time, and now it works hand-in-hand with our CDN across our whole digital ecosystem. With Kasada we are getting the service and outcomes that we need."

ABOUT KASADA

Kasada has developed a radical approach to defeating automated threats based on its unmatched understanding of the human minds behind them. The Kasada platform overcomes the shortcomings of traditional bot management to provide immediate and enduring protection for web, mobile, and API channels. Its invisible, dynamic defenses provide a seamless user experience and eliminate the need for ineffective, annoying CAPTCHAs. Our team handles the bots so clients have the freedom to focus on growing their businesses, rather than defending it. Kasada is based in New York and Sydney, with operations in Melbourne, Boston, San Francisco, and London.